CrowdStrike CCCS-203b Exam Questions - Guaranteed Success

2026 Latest ITdumpsfree CCCS-203b PDF Dumps and CCCS-203b Exam Engine Free Share: https://drive.google.com/open?id=1jmP_vhuwXLyBSIwmQdGgEHO4sm7PqoL7

Do you want to find a job that really fulfills your ambitions? That's because you haven't found an opportunity to improve your ability to lay a solid foundation for a good career. Our CCCS-203b learning materials are carefully compiled by industry experts based on the examination questions and industry trends in the past few years. The knowledge points are comprehensive and focused. You don't have to worry about our learning from CCCS-203b Exam Question. We assure you that our CCCS-203b learning materials are easy to understand and use the fewest questions to convey the most important information.

CrowdStrike CCCS-203b Exam Syllabus Topics:

Topic	Details
Topic 1	• Runtime Protection: This domain focuses on selecting appropriate Falcon sensors for Kubernetes environments, troubleshooting deployments, and identifying misconfigurations, unassessed images, IOAs, rogue containers, drift, and network connections.
Topic 2	• Cloud Security Policies and Rules: This domain addresses configuring CSPM policies, image assessment policies, Kubernetes admission controller policies, and runtime sensor policies based on specific use cases.
Topic 3	• Remediating and Reporting Issues: This domain addresses identifying remediation steps for findings, using scheduled reports for cloud security, and utilizing Falcon Fusion SOAR workflows for automated notifications.
Topic 4	• Cloud Account Registration: This domain focuses on selecting secure registration methods for cloud environments, understanding required roles, organizing resources into cloud groups, configuring scan exclusions, and troubleshooting registration issues.

>> CCCS-203b Latest Exam Experience <<

CrowdStrike CCCS-203b Exam dumps 2026

Many people may worry that the CCCS-203b guide torrent is not enough for them to practice and the update is slowly. We guarantee you that our experts check whether the CCCS-203b study materials is updated or not every day and if there is the update the system will send the update to the client automatically. So you have no the necessity to worry that you don't have latest CCCS-203b Exam Torrent to practice. We provide the best service to you and hope you are satisfied with our CCCS-203b exam questions and our service.

CrowdStrike Certified Cloud Specialist Sample Questions (Q283-Q288):

NEW QUESTION # 283
While scanning a container image in the CrowdStrike Falcon platform, you need to identify all installed packages to verify their versions and check for vulnerabilities. Which approach provides the most accurate and efficient method for obtaining this information?

- A. Use the ls command within a running container to list all files and infer installed packages.
- B. Leverage the Falcon platform's image scanning feature to generate a software bill of materials (SBOM).
- C. Use a base image with fewer vulnerabilities and avoid scanning individual packages.
- D. Manually inspect the Dockerfile used to build the container image.

Answer: B

Explanation:
Option A: Although choosing a secure base image is a good practice, it does not eliminate the need for scanning. Vulnerabilities can exist in dependencies or added packages beyond the base image.
Option B: The ls command is not designed to provide package-specific information and is prone to errors. It cannot accurately determine installed package versions.
Option C: The Dockerfile may not reflect the final state of the image, as additional packages could be installed during runtime or through indirect dependencies.
Option D: The Falcon platform's scanning capability provides a detailed and accurate SBOM, including package names, versions, and associated vulnerabilities. This is the most efficient and reliable method.

NEW QUESTION # 284
A security team is tasked with ensuring that no Kubernetes workloads in the cluster can run as privileged containers. They decide to use an admission controller policy to enforce this restriction.
Which of the following policy configurations is the most appropriate?

- A. Use a Role-Based Access Control (RBAC) rule to prevent users from creating privileged pods
- B. Use a MutatingWebhookConfiguration to automatically change securityContext.privileged: true to false in pod specifications
- C. Use a NetworkPolicy to block network traffic from privileged pods
- D. Use a ValidatingWebhookConfiguration to check and deny any pod with securityContext.privileged:
  true

Answer: D

Explanation:
Option A: While a MutatingWebhookConfiguration can modify pod specifications, it is not ideal for security enforcement because attackers might still find a way to override or bypass it. A validating webhook provides stricter enforcement.
Option B: A ValidatingWebhookConfiguration allows for centralized policy enforcement and can explicitly reject requests that attempt to create privileged containers by checking securityContext.privileged.
Option C: RBAC rules control permissions for users and service accounts but do not enforce runtime security settings such as preventing privileged containers.
Option D: Network Policies are used to control communication between pods but do not restrict the creation of privileged containers.

NEW QUESTION # 285
While reviewing a container image for vulnerabilities, which of the following steps ensures that vulnerabilities in installed software packages are detected and addressed effectively?

- A. Running a static analysis scan on the container image.
- B. Relying on the image author's documentation to identify vulnerabilities.
- C. Checking for updates to the container orchestration platform.
- D. Comparing the image against a trusted, verified base image.

Answer: A

Explanation:
Option A: Image authors may provide useful information, but relying solely on their documentation is risky. They might not have updated their documentation with the latest vulnerability information, and the analysis would lack thoroughness.
Option B: While keeping the orchestration platform updated is important, this does not address vulnerabilities within the container image itself. The two are separate layers of the container ecosystem.
Option C: Static analysis scanning tools are purpose-built to analyze container images for vulnerabilities in installed packages, libraries, and dependencies. They use vulnerability databases (e.g., CVE databases) to identify known issues, enabling you to patch or replace insecure packages before deploying the image.
Option D: Comparing images can help identify deviations but does not specifically identify vulnerabilities in installed packages. A static analysis scan is more comprehensive and accurate for this purpose.

NEW QUESTION # 286
What is needed to achieve visibility into the latest AWS IAM 1020 restricted use of AWS CloudShell with the latest CIS Foundations Benchmarks for AWS, Azure, and Google Cloud?

- A. Create custom IOM policy
- B. Leverage existing IOA policy
- C. Leverage existing IOM policy
- D. Create custom IOA policy

Answer: C

Explanation:
Visibility intoAWS IAM controls, includingrestricted use of AWS CloudShell (CIS IAM 1.20), is provided throughCrowdStrike Falcon Cloud Security posture managementusingIndicators of Misconfiguration (IOMs). These checks continuously evaluate cloud resources againstindustry-standard benchmarks, including theCIS Foundations Benchmarks for AWS, Azure, and Google Cloud. CrowdStrike maintainsprebuilt, managed IOM policiesthat are automatically updated to reflect the latest CIS guidance. Leveraging existing IOM policies ensures immediate coverage without the operational risk or overhead of creating and maintaining custom rules. These policies assess IAM configurations, permissions usage, service access controls, and policy enforcement related to CloudShell usage.
IOAs are designed for runtime behavioral detections and are not suitable for posture or configuration validation. Creating custom IOMs is unnecessary for CIS-aligned controls because CrowdStrike already provides validated, benchmark-mapped policies maintained by CrowdStrike security research.
Therefore,leveraging existing IOM policiesis the correct and recommended approach to maintain continuous, benchmark-aligned visibilityacross multi-cloud environments.

NEW QUESTION # 287
Which method can be used to identify running processes in a cloud environment without deploying a Falcon sensor?

- A. SSH into each virtual machine to manually inspect running processes
- B. Rely on the built-in antivirus solutions of the cloud provider
- C. Deploy Falcon Discover for Cloud Environments
- D. Cloud-native tools like AWS CloudWatch, Azure Monitor, or Google Cloud Operations Suite

Answer: D

Explanation:

Option A: While Falcon Discover provides comprehensive visibility into cloud workloads, it requires deployment on monitored environments. The question specifies identifying running processes without deploying a Falcon sensor, so this option is invalid.
Option B: Manually SSHing into VMs to inspect processes is inefficient and does not scale in modern cloud environments. This method increases administrative overhead and risks configuration drift. Additionally, SSH access may not be available due to strict security policies.
Option C: Cloud-native monitoring tools like AWS CloudWatch, Azure Monitor, and Google Cloud Operations Suite allow visibility into running processes, system metrics, and logs without requiring third-party agents. These services can provide runtime data and integrate with CrowdStrike for deeper insights. They are essential for environments where agent installation is limited by operational constraints.
Option D: Built-in antivirus solutions, such as Microsoft Defender for Endpoint or AWS GuardDuty, focus on threat detection rather than providing detailed runtime process visibility.
These tools lack the specificity required to identify and monitor all running processes.

NEW QUESTION # 288
.....